Figure 1
(PRIOR ART)

Trusted Authority

Secret: s

Public: P, sP

1

IBC

Party B has identity ID and a secret S_{ID} from TA where
$S_{ID} = sQ_{ID}$ and $Q_{ID} = H_1 (ID)$

Encryption

Encryption by party A
with secret r
$U = rP$
$V = m \oplus H_3(t(sP, rQ_{ID}))$

Decryption by party B
$m = V \oplus H_3(t(U, S_{ID}))$

3

Signatures

Signing by Party B
$h = H_2(m\|r)$
where $r = t(S_{ID}, P)^k$
$U = (k-h)S_{ID}$
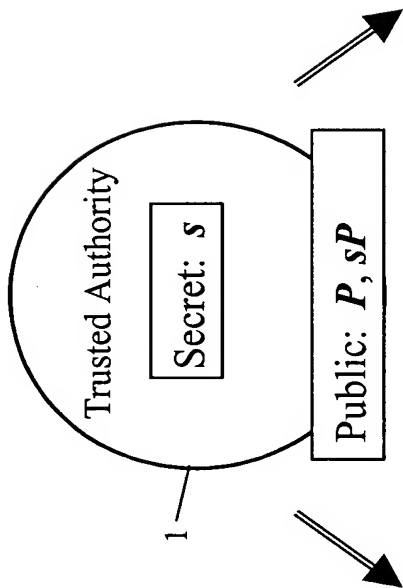
Verification by third party
$r' = t(U,P) * t(Q_{ID}, sP)^h$
Check
$h = H_2(m\|r')$

4

**Non IBC
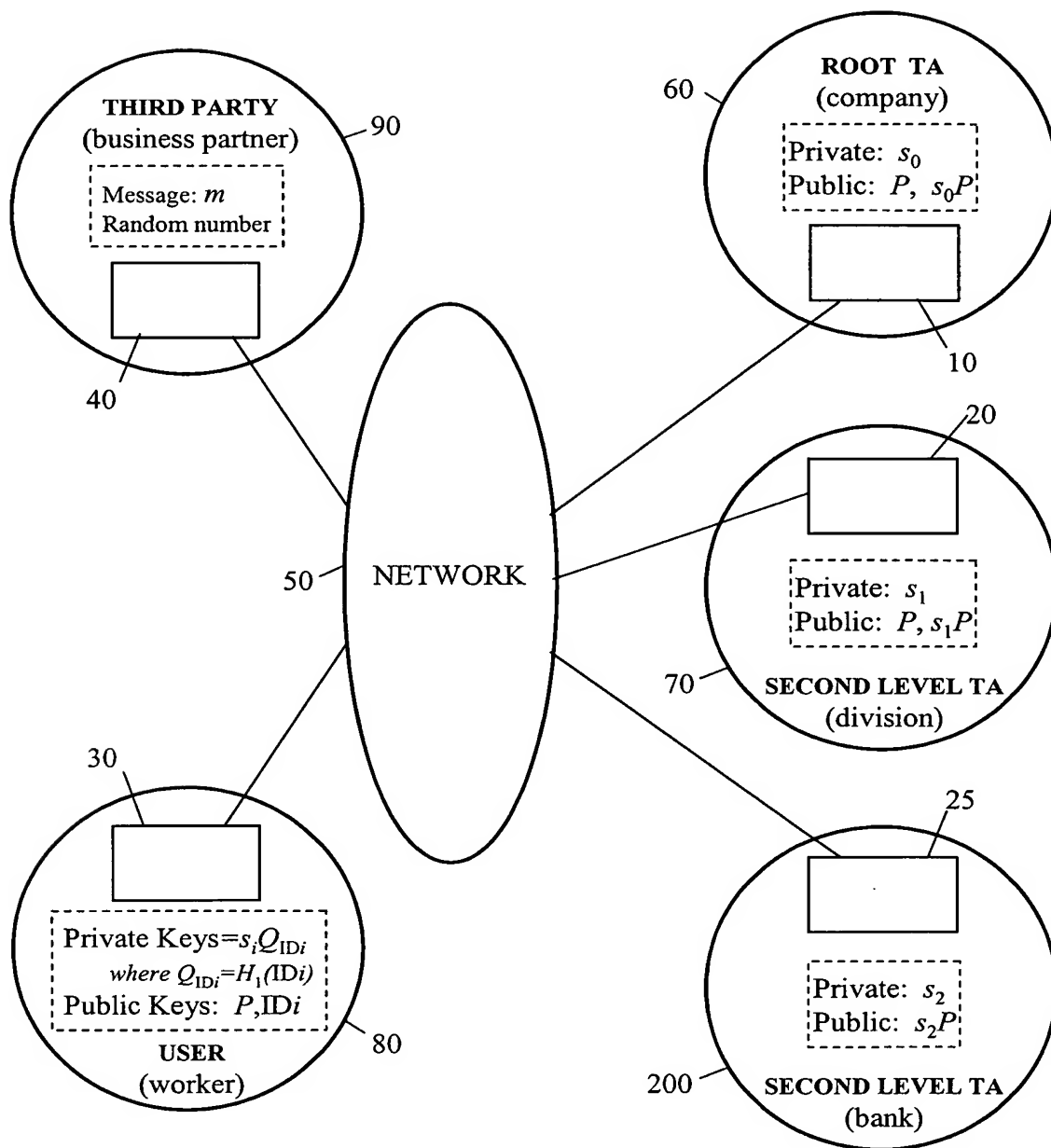Signatures**

Signing by TA:
$V = sH_1(m)$

Verification by third party
Check:
$t(P, V) = t(sP, H_1(m))$

2

2/3

THIRD PARTY
(business partner)

Message: m
Random number

90

40

ROOT TA
(company)

Private: s_0
Public: $P,\ s_0P$

60

10

NETWORK

50

20

Private: s_1
Public: P, s_1P

SECOND LEVEL TA
(division)

70

30

Private Keys$=s_iQ_{\mathrm{ID}i}$
where $Q_{\mathrm{ID}i}=H_1(\mathrm{ID}i)$
Public Keys: $P,\mathrm{ID}i$

USER
(worker)

80

25

Private: s_2
Public: s_2P

SECOND LEVEL TA
(bank)

200

Figure 2

3/3

Embodiment	Key Type	Identity Element	TA Element	Session Element	General Form
First	Encryption "Enc"	Q_{IDi} Public	R_{TAi} Public	r Private	$\prod t(R_{TAi}, rQ_{IDi})$
	Decryption "Dec"	S_{IDi} Private Q_{IDi} in S_{IDi}	s_i in S_{IDi}	U Public	$t(U, \sum b_i S_i)$
Second	Encryption "gID"	Q_{IDi} Public	P_{pubi} Public	σ Private	$\prod \hat{e}(Q_{IDi}, Ppubi)$
	Decryption "x"	d_{IDi} Private Q_{IDi} in d_{IDi}	s_i in d_{IDi}	U Public	$\hat{e}(\sum d_{IDi}, U)$
Third	Signature (compound)	d_{IDi} Private	P_{pubi} Public	z Private	$h \sum d_{IDi} + z \sum P_{pubi}$
	Verification (compound)	Q_{IDi} Public	P_{pubi}, U Public	U Public	$\prod \hat{e}(P_{pubi}, hQ_{IDi} + U)$
Fourth	Signature "e"	d_{IDi} Private Q_{IDi} in d_{IDi}	s_i in d_{IDi}	k Private	$\hat{e}(\sum d_{IDi}, P)$
	Verification ""e""	Q_{IDi} Public	P_{pubi} Public	h, S Public	$\prod \hat{e}(Q_{IDi}, P_{pubi})$

Figure 3